PERMISSION ANALYZER

USER MANUAL

Protect your data and get in control!

Scan your network, filter NTFS permissions,

validate your access control design

and trace user or group access.

PERDEMIASOFTWARE
Get in control

1. What is Permission Analyzer? 4
Main features 4
Scanning the network 4
Running your overviews 4
Tracing permissions 5
Creating reports and policies 5
2. Features 5
Scan your network 5
Configuring LDAP connections 5
Adding directories and LDAP OUs 6
Starting scan 7
Filters and overviews 8
Filter for users and groups 8
Filter for permission privileges 9
Filter for directories and files 10
Overview of permissions 10
Tracing permissions 12
Report and export 13
E-mail 13
Report templates 13
Filter selections 13
Running reports automatically 14
Report types 14
Manage reports 18
Quick export 18
Defining policies 18
Example 19
Schedule jobs 22
Modifying permissions 23
Data protection 24
External database 25
Other features 26
Show member info 26

Configuring LDAP attributes 28
Update service 28
3. Download 29
Version history 29
4. Licensing model 30
5. FAQ 32
Application queries 32
Licensing queries 33

1. What is Permission Analyzer?

Permission Analyzer scans your network and combines NTFS permissions with user and group data from the Active Directory. All data that is stored locally can be retrieved to create overviews of permissions per group or user. You will be able to monitor permissions for entire user groups and receive notifications if undesired permissions are flagged within your network.

MAIN FEATURES

Scanning the network

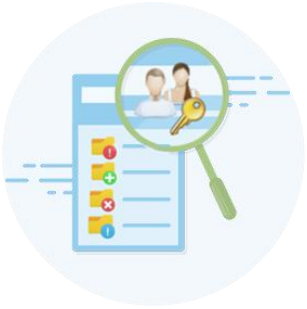
Configure the directories and LDAP Organizational Units to scan. All directory information and group memberships from LDAP are saved in a local database file. Run the scan whenever you like or schedule an automated scan. Permission Analyzer supports an external database, allowing multiple workstations to share the same information source.

Running your overviews

All information is saved on a database, allowing you to conduct targeted search queries in seconds, instead of scanning the whole network every time you want to apply a new filter. Add filters for specific members, all members of a group or LDAP OU, permissions or folders.

Tracing permissions

The main overview provides an aggregated summary of all permissions found and may contain the permissions of multiple users or groups. The Trace function is part of the overview and shows you the origin of permissions for a specific user or group and folder (via the group membership or parent folder they have been inherited). Use this view to zoom in on your search results.



Creating reports and policies

Save your filters as report and export them to HTML or CSV and e-mail. Use Permission Analyzer to run reports automatically using command-line parameters. Save your filters as policies and receive e-mail notifications if your policy report contains unwanted permissions.

2. Features

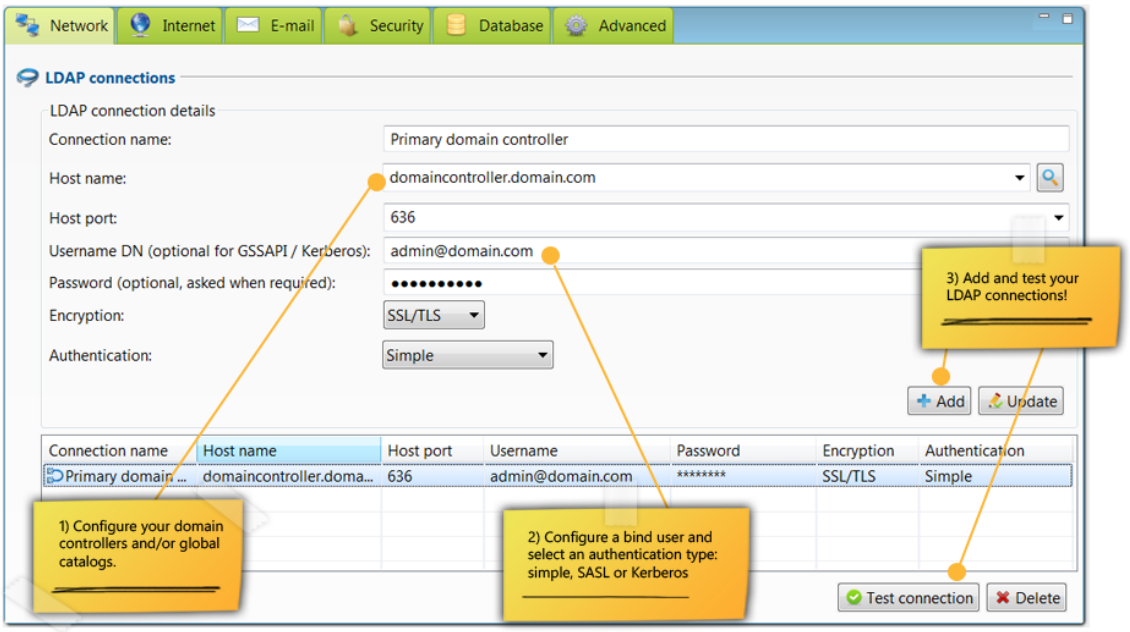
SCAN YOUR NETWORK

Specify directories or network shares to scan and configure depth. Add (nested) group membership information to the database by selecting particular LDAP Organizational Units to scan.

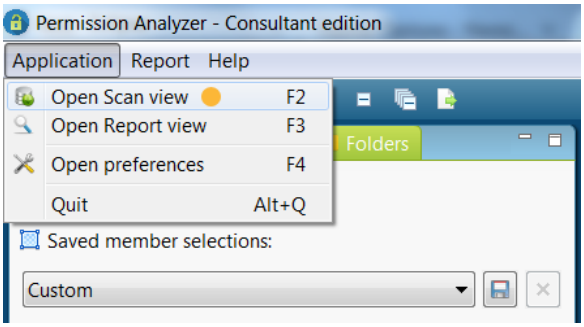
Permission Analyzer has two key functionalities: network scanning and overview creation. During the scanning process, all necessary information is stored in the corresponding local database. A major advantage of this feature, firstly, is that the network need not be overloaded with each overview that is run. Secondly, any overview results are available within a matter of seconds. The database contains the Access Control List of each folder (or file), group and user data from the LDAP, such as usernames, and data on (nested) group relations. In addition, Permission Analyzer supports a series of external databases, allowing data to be centralized and shared between multiple workstations. Please see chapter on External Database.

Configuring LDAP connections

Open **settings** and add the LDAP connections you wish to add, such as various domain controllers or a global catalog. Permission Analyzer supports multiple authentication protocols, such as (bind) username and password, Digest-MD5, Cram-MD5 or Kerberos. In addition, users can choose between plain, SSL/TLS or STARTTLS security protocols.



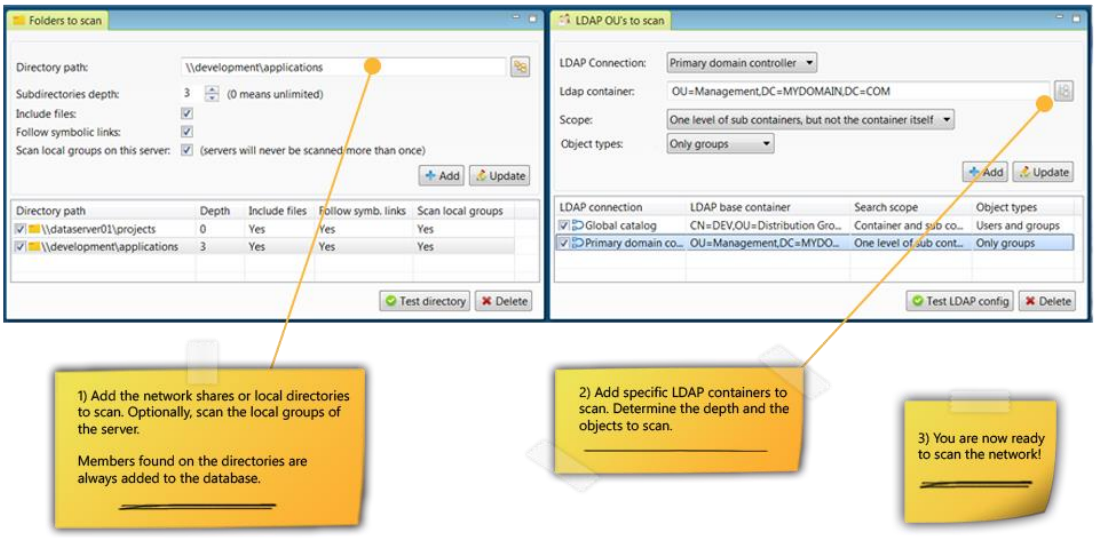
Adding directories and LDAP OUs



Open **Scan View** via the menu and determine which directories and LDAP Organizational Units (OU) need to be scanned by Permission Analyzer. LDAP OUs are used to supplement user data from the ACL with a username and nested group information for the relevant member.

Directories can be limited by setting up a depth limit for the number of subdirectories, file scanning and scanning of local groups on the server of the directory. LDAP OUs can also be configured with a depth limit as well as selected scanning of users and/or groups. Permission Analyzer will at all times ensure that a comprehensive overview of nested group data is available by assessing the **member** and **memberOf** attributes of each user or group. As such, the scan may expand beyond the selected OU.

Note: because a universal group can have members from domains other than the domain where the group object is stored and can be used to provide access to resources in any domain, only a global catalog server is guaranteed to have all universal group memberships that are required for authentication. On the other hand, the global catalog stores the membership (the member attribute) of only universal groups. The membership of other groups can be ascertained at the domain level. Therefore, if applicable, make sure you add both the domain controllers as your global catalogue to ensure a complete overview of group memberships. Permission Analyzer will make sure that no duplicate memberships are stored.

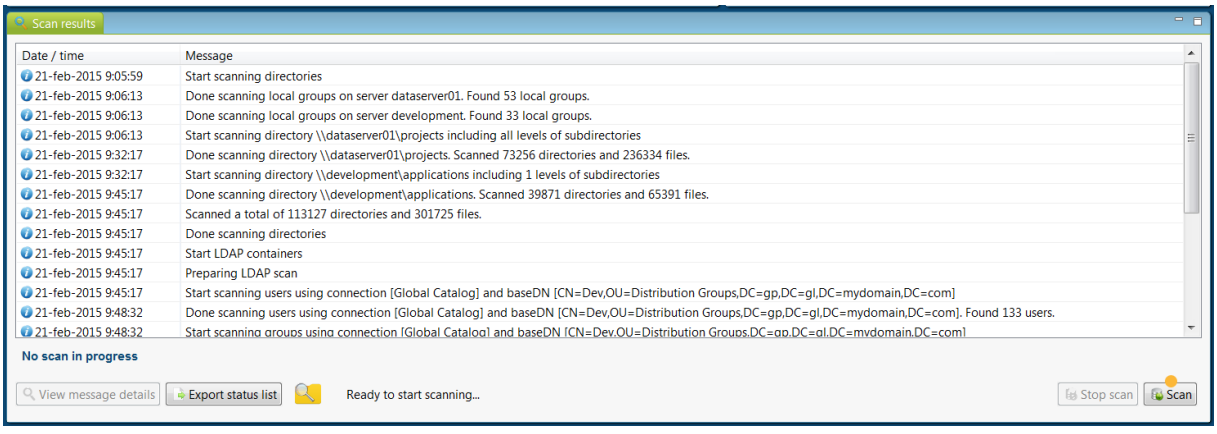


Starting scan

Permission Analyzer will refresh the database with the current network statistics when a scan is initiated. You will also be able to choose to refresh the databases or LDAP OUs only. This will result in the application leaving user and group data unchanged in the former and the directory data in the database unchanged in the latter. Only items that are **checked** will be scanned by Permission Analyzer.

A scan may be initiated automatically by the application using the scan parameter. The application will then commence a scan with the current configurations and subsequently close. An LDAP or directory scan may be initiated using the **-scanLDAP** or **-scanDirectories** parameters.

You will be able to review the results of the final scan in the status list or in the *Last_status_messages.csv* file in the application directory.

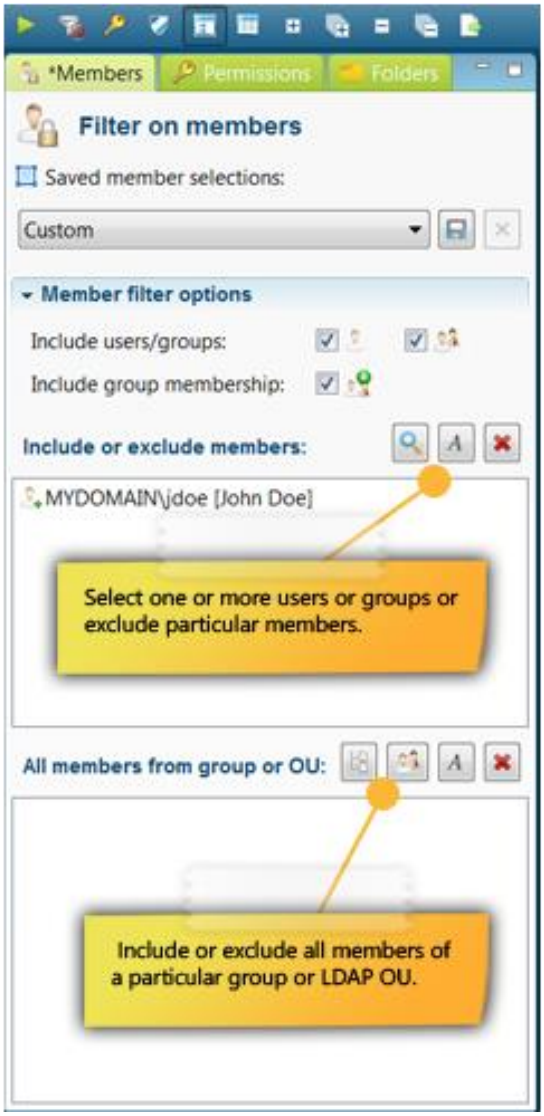

Scan results
Date / time
Message
21-feb-2015 9:05:59
Start scanning directories
21-feb-2015 9:06:13
Done scanning local groups on server dataserver01. Found 53 local groups.
21-feb-2015 9:06:13
Done scanning local groups on server development. Found 33 local groups.
21-feb-2015 9:06:13
Start scanning directory \\dataserver01\projects including all levels of subdirectories
21-feb-2015 9:32:17
Done scanning directory \\dataserver01\projects. Scanned 73256 directories and 236334 files.
21-feb-2015 9:32:17
Start scanning directory \\development\applications including 1 levels of subdirectories
21-feb-2015 9:45:17
Done scanning directory \\development\applications. Scanned 39871 directories and 65391 files.
21-feb-2015 9:45:17
Scanned a total of 113127 directories and 301725 files.
21-feb-2015 9:45:17
Done scanning directories
21-feb-2015 9:45:17
Start LDAP containers
21-feb-2015 9:45:17
Preparing LDAP scan
21-feb-2015 9:45:17
Start scanning users using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]
21-feb-2015 9:48:32
Done scanning users using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]. Found 133 users.
21-feb-2015 9:48:32
Start scanning groups using connection [Global Catalog] and baseDN [CN=Dev,OU=Distribution Groups,DC=gp,DC=gl,DC=mydomain,DC=com]
No scan in progress
View message details
Export status list
Ready to start scanning...
Stop scan
Scan

FILTERS AND OVERVIEWS

Create filters and include or exclude particular members, simple or special permissions and folders or files. Save your filters as Selection or save and re-use them as report.

Following the network scan, the database may be used to carry out search queries. Permission Analyzer offers an extensive set of filters for you to obtain specific information. The search results are represented in the **tree** structure or **table** of directories and files. An **aggregated** list of privileges is shown for each of the directories or files, as the search result(s) may contain privileges of multiple users or groups. You will be able to zoom in on the aggregated privileges using the Trace View feature at the bottom of the result window.

Filter for users and groups



The simplest filter displays the permission privileges for a specific group or user (hereafter to be referred to as **member**). The filter takes into account the nested group membership of the selected member. Permission Analyzer also allows for multiple members to be included in a single overview. Simply select **all members** of a specific group or LDAP OU or search using a **wildcard** key word for the account name and display name. This will allow you to monitor whether someone from a specific group has too many permission privileges in certain folders.

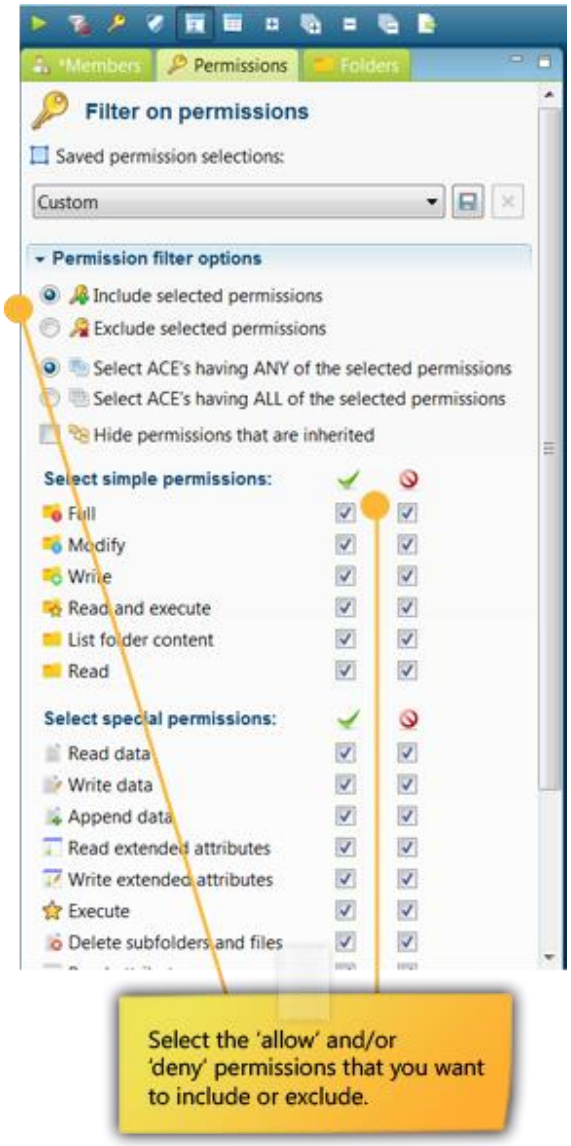
In addition to including members in searches, you are also able to **exclude** one or more members from searches, e.g. by excluding everyone from the Domain Admins group.

Filter for permission privileges

All permission privileges are automatically shown for each search. However, a filter can be created to **include** or **exclude** certain privileges from a search. The filter overview distinguishes between Windows simple permissions, special permissions or permissions that allow or deny something.

When filtering permission privileges you can indicate whether a member should have **all** privileges or **at least one** of those you have selected. The former can be used to filter for members with specific permissions (such as FULL), while the latter can be used to display a series of permissions.

If necessary, configure the filter to only display **explicit** permissions.



Filter for directories and files

Search results can be scoped to exclude certain directories or files. Adding a directory will automatically include all subdirectories and files. You will also be able to search for the name of a file or directory using a wildcard.

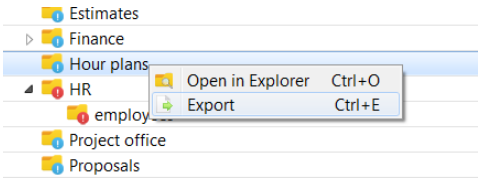
Tip: To retrieve a directory or file in the main window, use the Quick File Search box.

A set of filters can be saved as a **Selection**, making a large number of frequently used filters easily retrievable and usable. A selection will bundle filters of the same type (members, permissions or folders). The total number of filters for an overview can be saved as a Report. Filters can be modified by clicking **Run** and can be reset by clicking **Reset** in the toolbar.

Overview of permissions

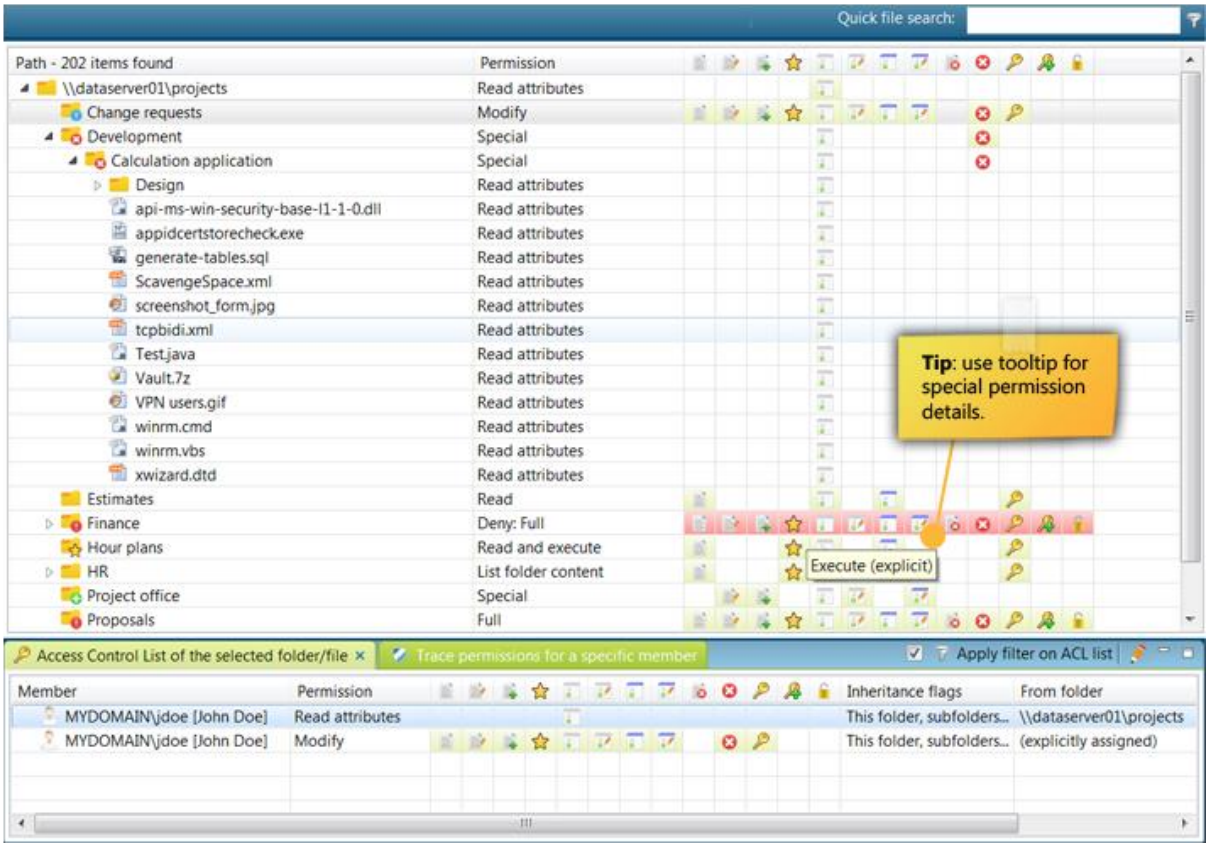
After applying the filters, all retrieved permissions will be shown in a tree structure, grouped in directories and files. The toolbar also contains an option to have results displayed in a table rather than a tree structure. Each item will contain a label with the relevant permission and a number of columns showing which special permissions apply e.g. permissions of various members, as each row is a sum of all retrieved permissions. The background color of the permissions indicates whether a permission was granted directly or if it was inherited from a folder above: white for implicit ‘allow’ permissions, green for explicit ‘allow’ permissions, light red for implicit ‘deny’ permissions and dark red for explicit ‘deny’ permissions.

Tip: Each directory within the search results can be exported to an HTML report or CSV file by opening the context menu with the right mouse button. Directories can also be opened directly with **Windows Explorer**.



There are two tabs at the bottom of the search result screen: one that provides details on the Access Control List of the directory selected and another which allows you to zoom in on a direct to review which permissions and members have been found. For more details see the Modifying permissions and Tracing permissions features.

Tip: drag tabs to a second screen or to another location within the application to view both tabs simultaneously.

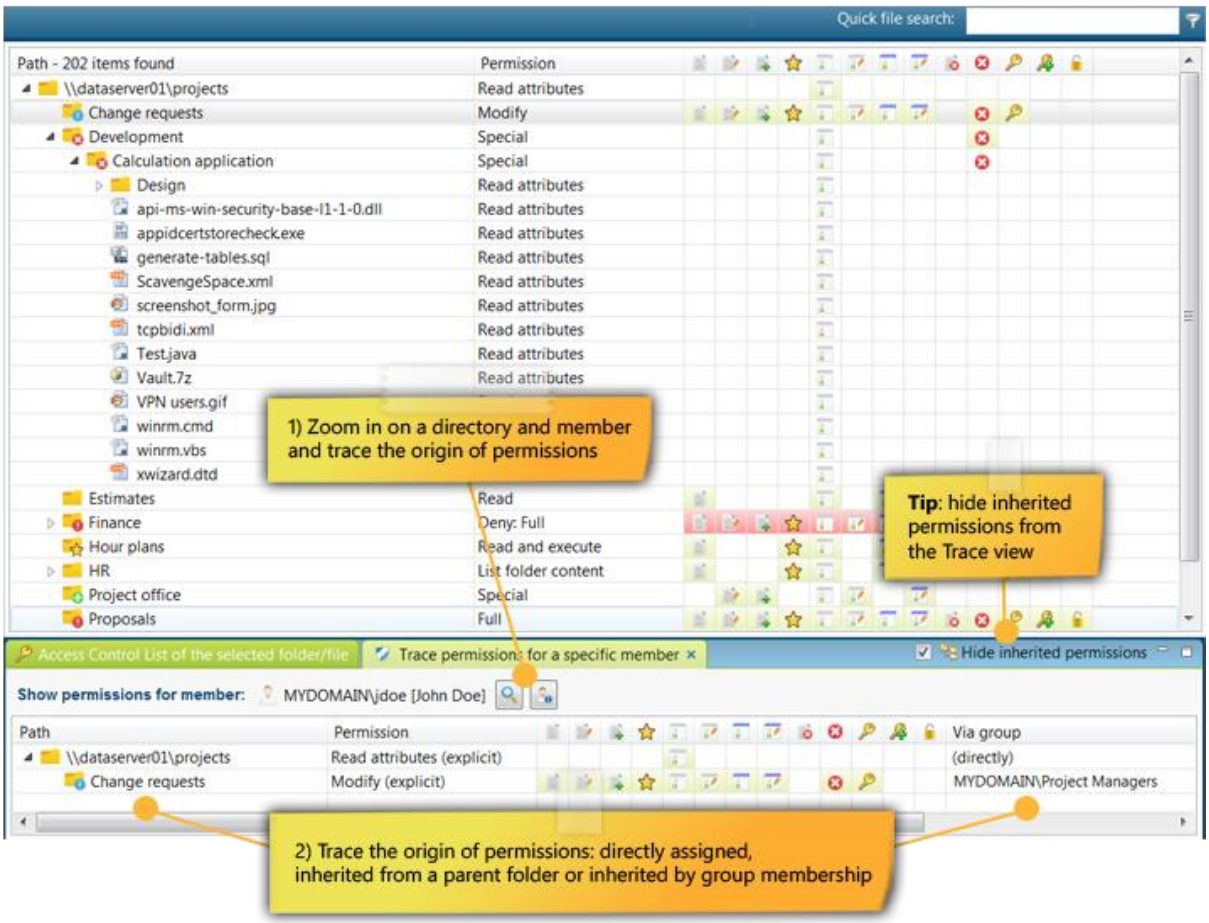


TRACING PERMISSIONS

Zoom in on your search results and trace the origin of permissions that have been found. See if permissions are inherited from a (indirect) group membership or parent folder.

To review a directory for all found permissions, see the tab at the bottom of the search result screen. Each directory in the main search result screen represents the **sum** of all permissions found. Should the filter criteria yield multiple members, then you may use Trace view to select a specific member. When selecting members, a list will be displayed only containing members for whom permissions have been found. The view subsequently displays all permissions that apply to that specific member as well as the provenance of those permissions, e.g. through which (nested) group membership or superior directory the permissions were granted. This feature allows you to easily track the cause of undesirable permissions and resolve such cases by modifying the permissions in ACL view.

Tip: Use the info button to get the group information of the member selected.



REPORT AND EXPORT

Save your filters as report and export them to HTML or CSV and e-mail. Use different report types, such as permissions tracing and group memberships, effective permissions or plain Access Control List information of your directories.

Current sets of filters can be saved as a new report using the menu [Report] > [Create new report]. Reports can be exported to **HTML** or **CSV** files or can be reloaded within the program to change the filters or review results. There are two options for HTML: a simple HTML table and an option which includes search, paging and sorting options.

E-mail

A report can be configured with an e-mail address, allowing it to be sent to that address at every export opportunity. An **SMTP** server, however, must be configured to accommodate the address and can be set up in the application settings. The option will also allow you to indicate whether you want the report to be included as an **attachment** and to include a message in the e-mail. The e-mail template may contain the following fields: `[report_name]`, `[report_path]`, `[report_description]` and `[report_threshold]`. The *file/folder count threshold* value in the report can be used to determine whether only to e-mail the report if it contains a certain number of folders or files. This can be used to create policies – see Defining Policies feature for more details.

Report templates

You will also be able to use modified templates to generate the report. Permission Analyzer comes with a number of default templates for HTML and CSV, which can be modified according to your specifications. The templates are located in *<application dir>\plugins\Permission_Analyzer_2.xxxx.jar* – the file can be opened with any ZIP application. Here are examples of an HTML template for effective permissions and a CSV template for ACL information.

Filter selections

If you have selected a filter selection as a filter, then that selection will show up as an option when generating the report. Using the selection will create a **reference** to the filter selection within the report and any modifications to the filter selection will result in all reports automatically applying the modified selection. Unchecking the option in the report will result in the report saving a **copy** of the filters and not change according to the filter selection.

Running reports automatically

Use Permission Analyzer to run reports automatically using the following parameters:

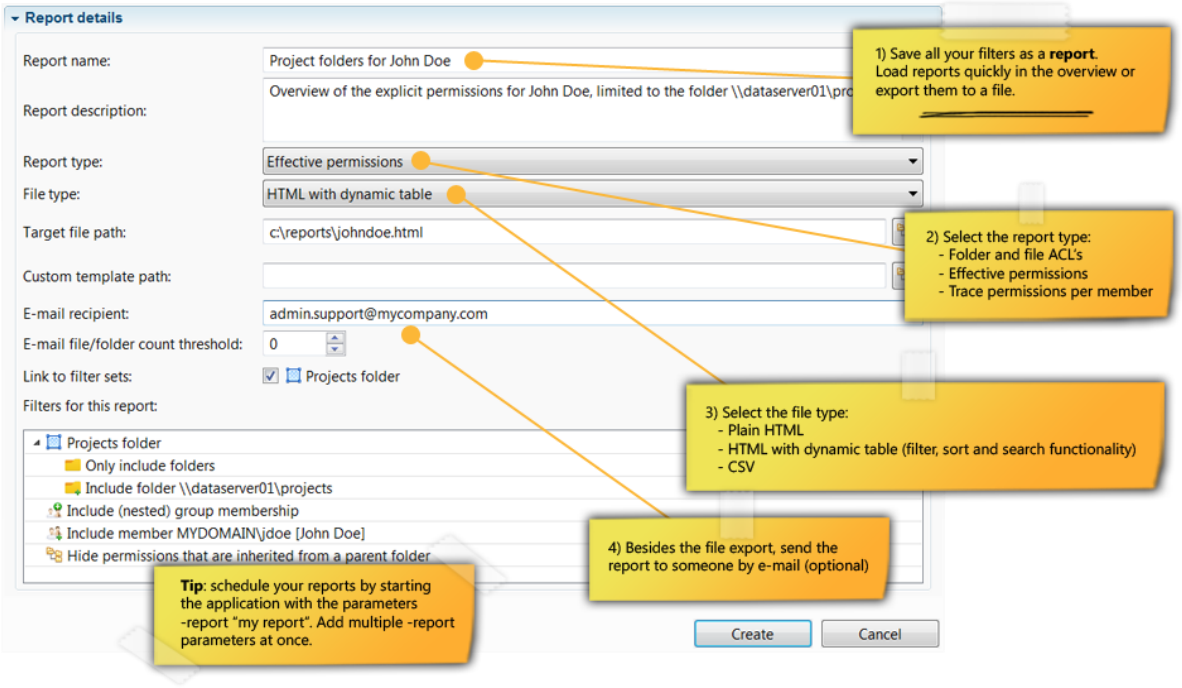
- **-report "myReport"**: run a specific report by name. This parameter can be input a number of times.
- **-allReports**: run all reports.
- **-allPolicies**: run all reports with a *file/folder count threshold* value greater than 0.

Permission Analyzer will close automatically after all reports have been exported. See Schedule jobs feature for more command-line options.

Report types

Permission Analyzer supports three report types, each of which displays search results differently:

- The ACL information of folders and files as they appear on the file system.
- Permissions tracing to show the origin of permissions per user.
- Effective permissions per user and folder or file, including permissions from nested group memberships.


Report details
Report name:
Project folders for John Doe
Report description:
Overview of the explicit permissions for John Doe, limited to the folder \\dataserver01\pro
Report type:
Effective permissions
File type:
HTML with dynamic table
Target file path:
c:\reports\johndoe.html
Custom template path:
E-mail recipient:
admin.support@mycompany.com
E-mail file/folder count threshold:
0
Link to filter sets:
Projects folder
Filters for this report:
Projects folder
Only include folders
Include folder \\dataserver01\projects
Include (nested) group membership
Include member MYDOMAIN\jdoe [John Doe]
Hide permissions that are inherited from a parent folder
1) Save all your filters as a report. Load reports quickly in the overview or export them to a file.
2) Select the report type:
- Folder and file ACL's
- Effective permissions
- Trace permissions per member
3) Select the file type:
- Plain HTML
- HTML with dynamic table (filter, sort and search functionality)
- CSV
4) Besides the file export, send the report to someone by e-mail (optional)
Tip: schedule your reports by starting the application with the parameters -report "my report". Add multiple -report parameters at once.
Create
Cancel

Tip: put a placeholder in the *Target file path* to include a current date in the path c:\reports\[date:yyyy-MM-dd]_report.html. Also see Java date formats.

FOLDER AND FILE ACLS

This report provides an overview of the Access Control Lists (ACL) per directory or file and contains all Access Control Entries (ACE) that match the search criteria. Each ACE has a set of permissions and a member and match the data in the **Windows Security tab** on the file properties. Only the directories and files that match the search criteria will be included in the report.

Directories and files found: 49

PERMISSION ANALYZER - ACL REPORT

The ACL report displays permission information that corresponds with the Access Control Lists on the file system. Only the members that match the selected filter criteria are displayed in the report.

ACL information of the projects folder.

Filters applied:

Include (nested) group membership
Include member MYDOMAIN\jdoe [John Doe]

Column visibility:

File path
Members
Permission text
Special permission
ACE flags
Inherited from folder

Show 50 entries

Search:

Member	Permission	Read data	Write data	Append data	Execute	Read attributes	Write attributes	Read extended attributes	Write extended attributes	Delete subfolders and files	Delete	Read permissions	Change permissions	Take ownership	ACE flags	Inherited from folder
\\dataserver01\projects																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	(explicitly assigned)
\\dataserver01\projects\Change requests																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	\\dataserver01\projects
MYDOMAIN\jdoe [John Doe]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	(explicitly assigned)
\\dataserver01\projects\Development																
MYDOMAIN\jdoe [John Doe]	Delete										✓				This folder, subfolders and files (no propagate)	(explicitly assigned)
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	\\dataserver01\projects
\\dataserver01\projects\Development\Calculation application																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	\\dataserver01\projects
MYDOMAIN\jdoe [John Doe]	Delete										✓				This folder only	\\dataserver01\projects\Development
\\dataserver01\projects\Development\Calculation application\appidcertstorecheck.exe																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This file only	\\dataserver01\projects
\\dataserver01\projects\Development\Calculation application\Design																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	\\dataserver01\projects
\\dataserver01\projects\Development\Calculation application\Design\clfs.sys																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This file only	\\dataserver01\projects
\\dataserver01\projects\Development\Calculation application\Vault.7z																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This file only	\\dataserver01\projects
\\dataserver01\projects\Development\Calculation application\xwizard.dtd																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This file only	\\dataserver01\projects
\\dataserver01\projects\Estimates																
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓						✓	✓			This folder, subfolders and files	\\dataserver01\projects
MYDOMAIN\jdoe [John Doe]	Read	✓				✓		✓				✓			This folder, subfolders and files	(explicitly assigned)
\\dataserver01\projects\Finance																
MYDOMAIN\jdoe [John Doe]	Special	✓			✓						✓				This folder, subfolders and files	(explicitly assigned)
MYDOMAIN\Freelancers [global group]	Deny: Modify	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			This folder, subfolders and files	(explicitly assigned)
MYDOMAIN\Project Managers [global group]	Modify	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓			This folder, subfolders and files	\\dataserver01\projects
\\dataserver01\projects\Website\Clients																
MYDOMAIN\jdoe [John Doe]	Take ownership													✓	Subfolders and files only (not this folder)	(explicitly assigned)
\\dataserver01\projects\Website\Clients\Content																
MYDOMAIN\jdoe [John Doe]	Take ownership													✓	This folder, subfolders and files	\\dataserver01\projects\Website\Clients\Content
MYDOMAIN\Content Managers [global group]	Write attributes						✓		✓						This folder, subfolders and files	(explicitly assigned)

Showing 1 to 50 of 89 entries

Previous 1 2 Next

TRACE PERMISSIONS

Trace reports show the origin of permissions per group or user, indicating through which (nested) group a user or group has inherited those permissions. Only users and groups that appear in the search results will be included in the report. A report shows a relatively extensive amount of information per user and group. That's why we recommend making your filters as specific and targeted as possible, to exclude any unnecessary information. This prevents reports from being crowded with irrelevant information.

Directories and files found: 15

PERMISSION ANALYZER - TRACE REPORT

Project folders for John Doe

The Trace report displays permission information for all members that match the selected filter criteria. For each member the report will show all applicable Access Control Entries and where they come from, meaning via what group membership.

Explicit permissions for John Doe scoped on the projects folder

Filters applied:

- Include (nested) group membership
- Include member MYDOMAIN\jdoe [John Doe]
- Hide permissions that are inherited from a parent folder
- Include folder \\dataserver01\projects

Column visibility:

- File path
- Members
- Permission text
- Special permission
- ACE flags
- Via group

Show 50 entries Search:

Member	Permission	Read data	Write data	Append data	Execute	Read attributes	Write attributes	Read extended attributes	Write extended attributes	Delete subfolders and files	Delete	Read permissions	Change permissions	Take ownership	Via group	ACE flags
\\dataserver01\projects																
MYDOMAIN\jdoe [John Doe]	Read attributes (explicit)					✓									MYDOMAIN\Project Managers [global group]	This folder, subfolders and files
\\dataserver01\projects\Change requests																
MYDOMAIN\jdoe [John Doe]	Modify (explicit)	✓	✓	✓	✓	✓	✓	✓	✓		✗	✓			MYDOMAIN\Planning [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development																
MYDOMAIN\jdoe [John Doe]	Delete (explicit)										✗				MYDOMAIN\Programmers [global group]	This folder, subfolders and files (no propagate)
\\dataserver01\projects\Estimates																
MYDOMAIN\jdoe [John Doe]	Read (explicit)	✓				✓		✓				✓			MYDOMAIN\Project managers [global group]	This folder, subfolders and files
\\dataserver01\projects\Finance																
MYDOMAIN\jdoe [John Doe]	Deny: Full (explicit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	MYDOMAIN\Freelancers [global group]	This folder, subfolders and files
MYDOMAIN\jdoe [John Doe]	Special (explicit)	✓			✓						✗				(direct)	This folder, subfolders and files
\\dataserver01\projects\Intranet\Apps																
MYDOMAIN\jdoe [John Doe]	Write attributes (explicit)						✓								(direct)	This folder, subfolders and files
\\dataserver01\projects\Intranet\Infra																
MYDOMAIN\jdoe [John Doe]	Special (explicit)		✓	✓		✓	✓	✓	✓	✓	✗	✓	✓	✓	MYDOMAIN\Intra Support [global group]	This folder, subfolders and files
\\dataserver01\projects\Intranet\Departments																
MYDOMAIN\jdoe [John Doe]	Special (explicit)			✓							✗				MYDOMAIN\Content Managers [global group]	This folder, subfolders and files
\\dataserver01\projects\Website\Clients																
MYDOMAIN\jdoe [John Doe]	Take ownership (explicit)													✓	(direct)	This folder, subfolders and files
\\dataserver01\projects\Website\Content																
MYDOMAIN\jdoe [John Doe]	Delete (explicit)										✗				MYDOMAIN\Content Managers [global group]	This folder, subfolders and files
\\dataserver01\projects\Hour plans																
MYDOMAIN\jdoe [John Doe]	Read and execute (explicit)	✓			✓	✓		✓				✓			MYDOMAIN\Planning [domain local group]	This folder, subfolders and files
\\dataserver01\projects\HR																
MYDOMAIN\jdoe [John Doe]	List folder content (explicit)	✓			✓	✓		✓				✓			MYDOMAIN\HR Admins [global group]	This folder and subfolders
\\dataserver01\projects\Project office																
MYDOMAIN\jdoe [John Doe]	Write (explicit)		✓	✓			✓		✓						MYDOMAIN\Project Admins [global group]	This folder, subfolders and files
\\dataserver01\projects\Proposals																
MYDOMAIN\jdoe [John Doe]	Full (explicit)	✓	✓	✓	✓	✓	✓	✓	✓	✓	✗	✓	✓	✓	(direct)	This folder, subfolders and files

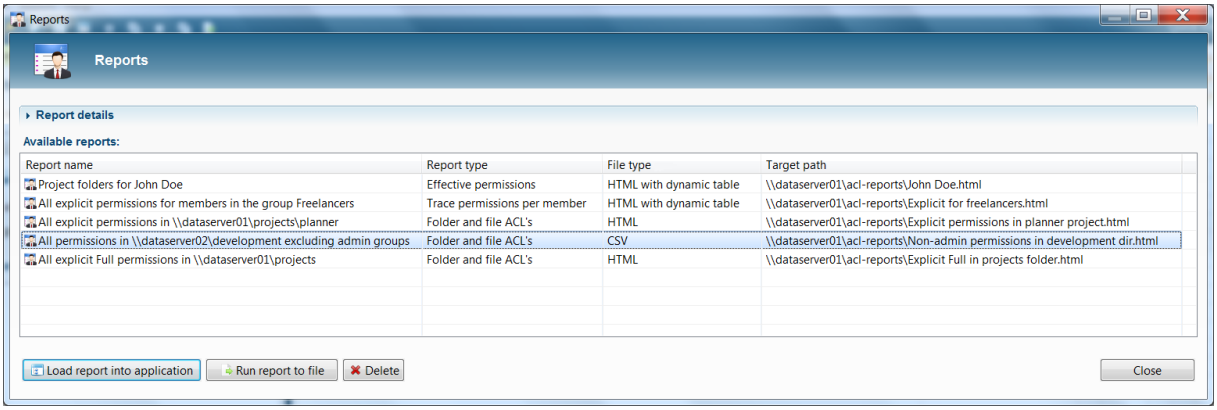
Showing 1 to 15 of 15 entries Previous 1 Next

EFFECTIVE PERMISSIONS

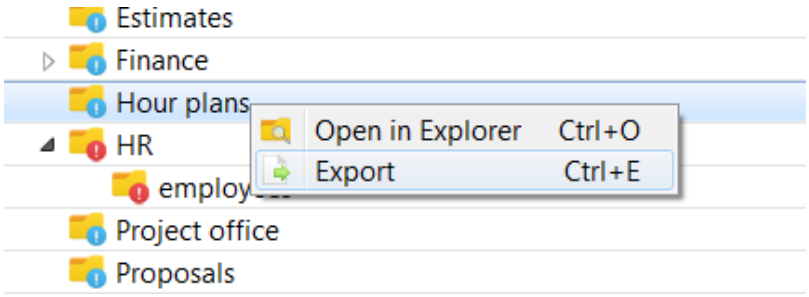
This report type shows a sum of all permissions found per directory or file and takes into account the priorities used by Windows (privileges that deny something will, for example, have a higher priority than privileges that grant access).

Manage reports

A list of all reports can be requesting via the menu: [Report] > [Manage Report]. You will subsequently be able to review and modify all reports, run them manually or input them into the application.



Quick export



Specific folders can be easily exported using the filters selected and will not require generation of a report. Simply open the context menu of a folder using the right mouse button and select Export. This option will also allow you to select the report type, file type and whether you wish to send an e-mail.

DEFINING POLICIES

Save your filters as policies and receive e-mail notifications if your policy report contains unwanted permissions.

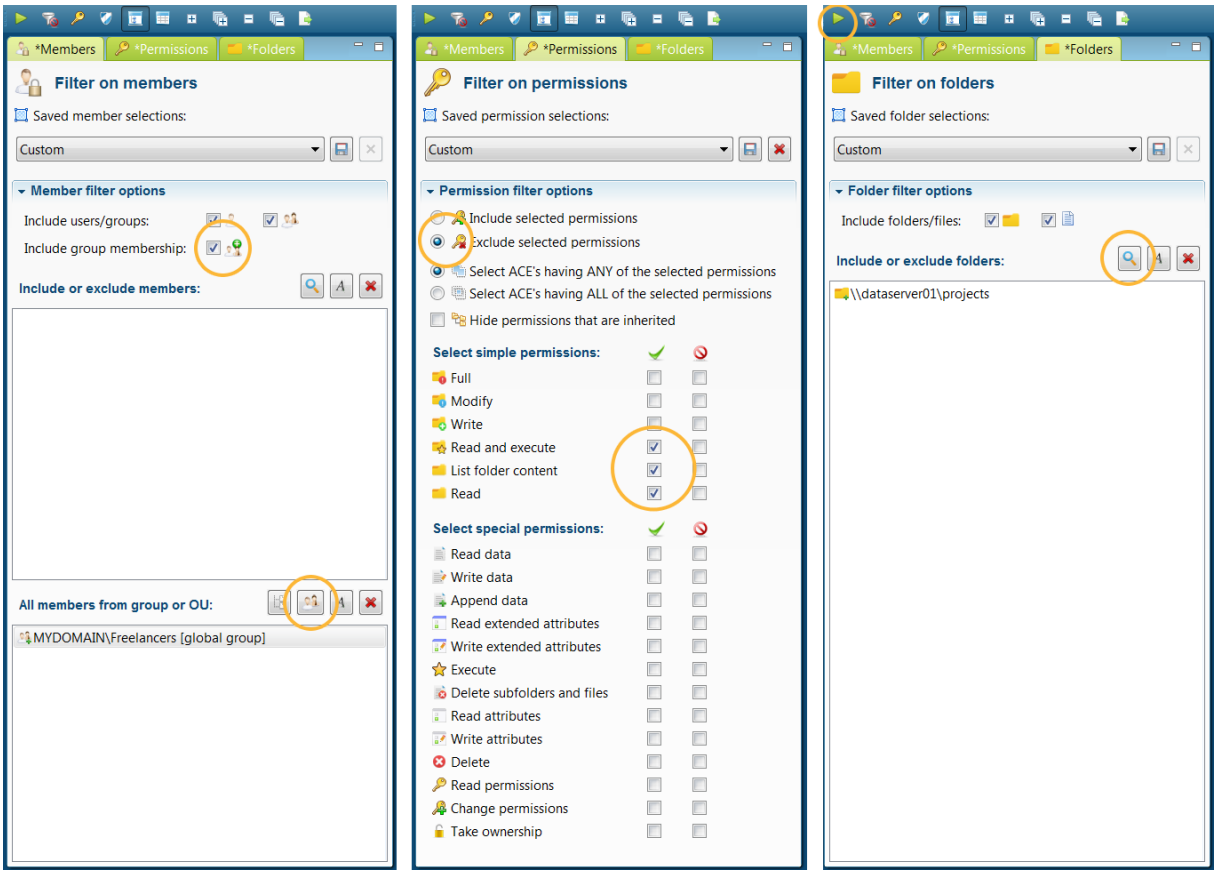
A policy is a collection of filters that display unwanted permissions. This collection can be saved as a report where an e-mail notification is sent if the report contains more than a certain number of directories and files. That number can be configured via the ***E-mail file/folder count threshold*** value in the report. Here's the difference between a policy report and a standard report: a policy report defines a combination of filters that should not yield any results. If any results are found, however, an e-mail notification is sent out. Running a policy report automatically from time to time will allow you to check for any unwanted permissions within the network. Also see the Schedule Jobs and Report and Export features.

A **SMTP** server should be configured to facilitate any e-mail notifications. Go to settings to configure the server. You will also be able to indicate whether you want the report to be included as an **attachment** and to include a message in the e-mail. The e-mail template may contain the following fields: `[report_name]`, `[report_path]`, `[report_description]` and `[report_threshold]`.

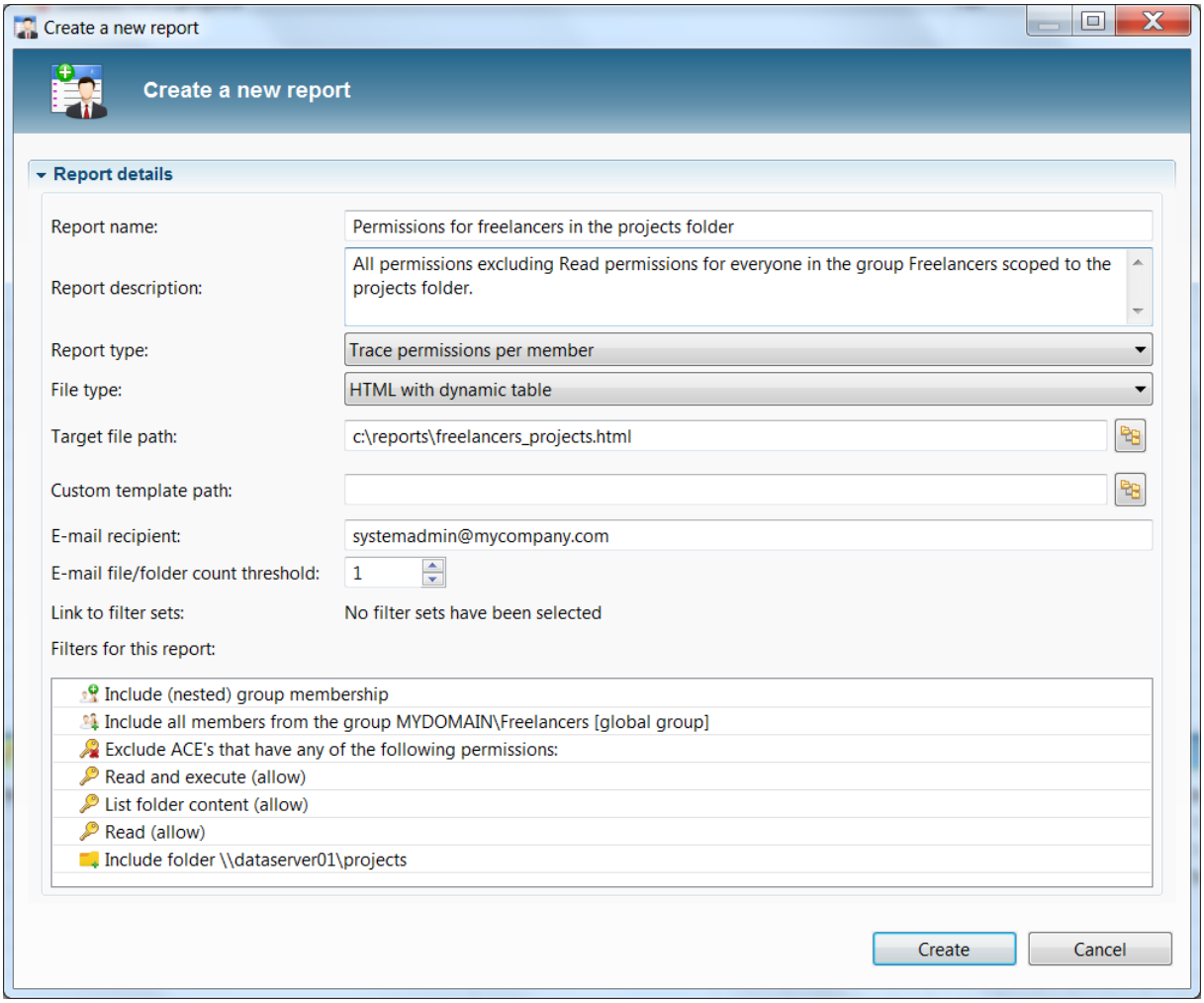
Example

If, in your access control design you determined that all freelancers within your network should be unable to modify project information and you would like to verify that policy with current permissions within the network. All freelancers are located in a communal group; project information is kept in the projects folder on a data server. First you will have to define the filters that make up the policy:

- Select Freelancers from the Members tab and add this group to the bottom selection list (see screenshot). This will not filter for the group itself but for **all** the members of that group. Nested group membership will automatically be taken into account for each group member when determining permissions.
- In the Permissions tab select the Exclude option and select all reading privileges. These, after all, are privileges that Freelancers have been granted and as such should be excluded from the policy report.
- In the Folders tab select the \\dataserver01\projects folder. Your search results will then be scoped to that specific folder.



Review your search results by applying the filters using the **Run** button. If necessary, add new filters, e.g. an Exclude filter for one or more users. Ideally, the result field will remain empty, meaning that no unwanted permissions have been found and that your policy has been implemented completely. Should you have any search result items that appear as exceptions, then simply raise the threshold value for e-mail notification in the report. The threshold value determines the number of files or folders notifications that are sent and can be configured in the *E-mail file/folder count threshold* field. At value 0 an e-mail is sent out every time a report is run, however, for a policy you will only want a notification if a minimum number of files is found, so you would set the value at 1 or more. Once your search results are satisfactory, save your filters as a new report.



The way a policy report is shown depends on the **report type** you selected – see Report and Export feature. If you selected a Trace report, it may look like the figure below. The report below shows that John Doe has Modify privileges in the “project\Change requests” through the “Project Office” group. It also shows Jane Murphy has full privileges within the “projects\Development” folder, as she is part of the “Testers”

group. These results show you who has acquired more permissions than is desirable and where additional permissions have been granted.

Directories and files found: 10

PERMISSION ANALYZER - TRACE REPORT

The Trace report displays permission information for all members that match the selected filter criteria. For each member the report will show all applicable Access Control Entries and where they come from, meaning via what group membership.

All permissions excluding Read permissions for everyone in the group Freelancers scoped to the projects folder.

Filters applied:

- Include (nested) group membership
- Include all members from the group MYDOMAIN\Freelancers [global group]
- Exclude ACE's that have any of the following permissions:
  - Read and execute (allow)
  - List folder content (allow)
  - Read (allow)
- Include folder \\dataserver01\projects

Column visibility:

File path, Members, Permission text, Special permission, ACE flags, Via group

Show 200 entries — Search:

Member	Permission	Read data	Write data	Append data	Execute	Read attributes	Write attributes	Read extended attributes	Write extended attributes	Delete subfolders and files	Delete	Read permissions	Change permissions	Take ownership	Via group	ACE flags
\\dataserver01\projects\Change requests																
MYDOMAIN\jdoe [John Doe]	Modify (explicit)				★						⊗	🔑			MYDOMAIN\Project Office [global group]	This folder, subfolders and files
\\dataserver01\projects\Development																
MYDOMAIN\jmurphy [Jane Murphy]	Full (explicit)				★						⊗	🔑	🔑		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application\appidcertstorecheck.exe																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\Testers [domain local group]	This file only
\\dataserver01\projects\Development\Calculation application\Design																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\Testers [domain local group]	This folder, subfolders and files
\\dataserver01\projects\Development\Calculation application\Design\clfs.sys																
MYDOMAIN\jmurphy [Jane Murphy]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\Testers [domain local group]	This file only
\\dataserver01\projects\Finance																
MYDOMAIN\jdoe [John Doe]	Special (explicit)				★						⊗				(direct)	This folder, subfolders and files
\\dataserver01\projects\HR																
MYDOMAIN\jdoe [John Doe]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\HR Admins [global group]	This folder, subfolders and files
\\dataserver01\projects\HR\employees																
MYDOMAIN\jdoe [John Doe]	Change permissions (explicit)												🔑		(direct)	This folder and subfolders
MYDOMAIN\jdoe [John Doe]	Full (inherited)				★						⊗	🔑	🔑		MYDOMAIN\HR Admins [global group]	This folder, subfolders and files
\\dataserver01\projects\Proposals																
MYDOMAIN\jdoe [John Doe]	Modify (explicit)				★						⊗	🔑			(direct)	This folder, subfolders and files

Showing 1 to 11 of 11 entries — Previous 1 Next

SCHEDULE JOBS

Use command-line parameters to run a network scan or report export automatically. Let Permission Analyzer check all your policies and send out e-mail notifications by running the application with parameters and Windows Scheduler.

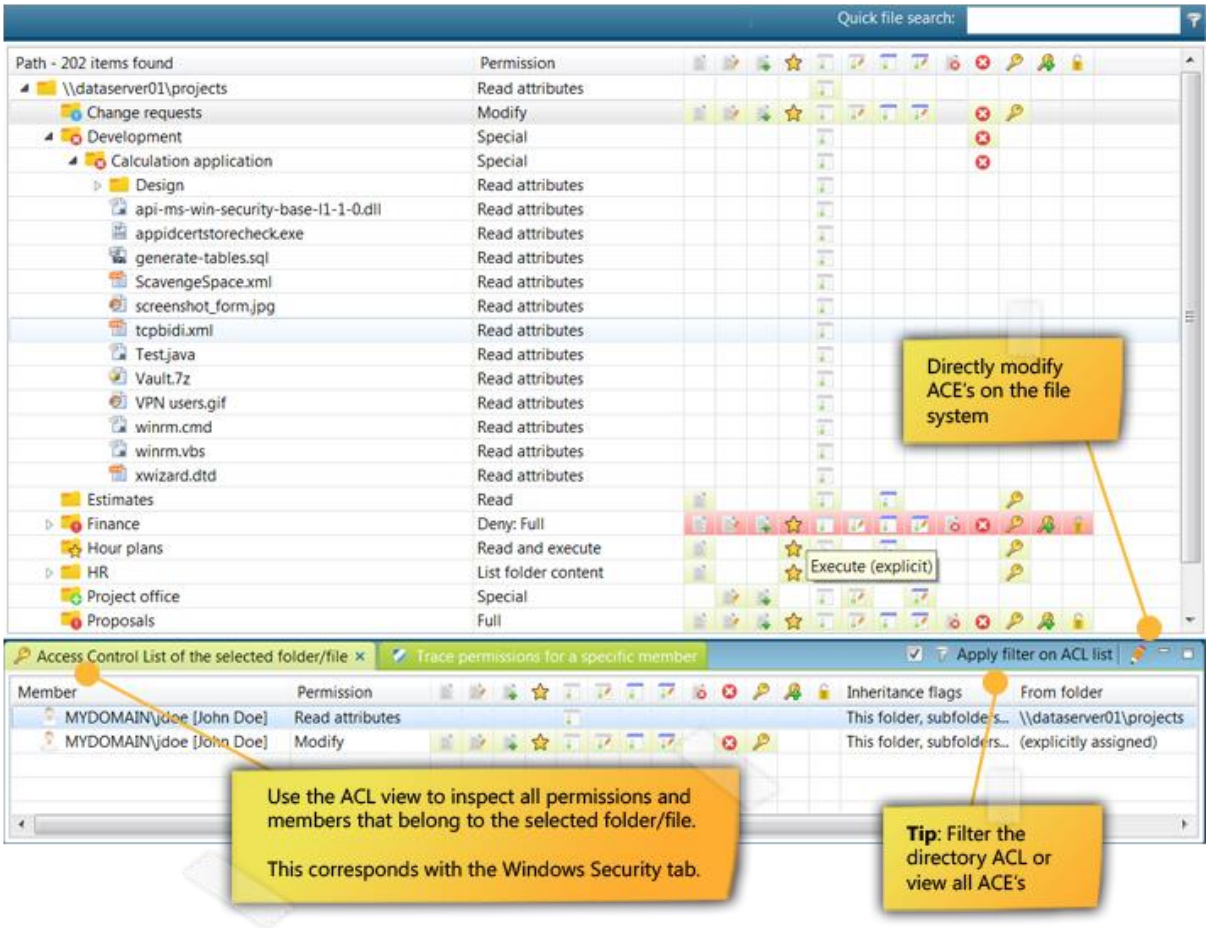
Permission Analyzer is able to run network scans and export reports automatically. Simply use Windows Scheduled Tasks and a combination of application parameters:

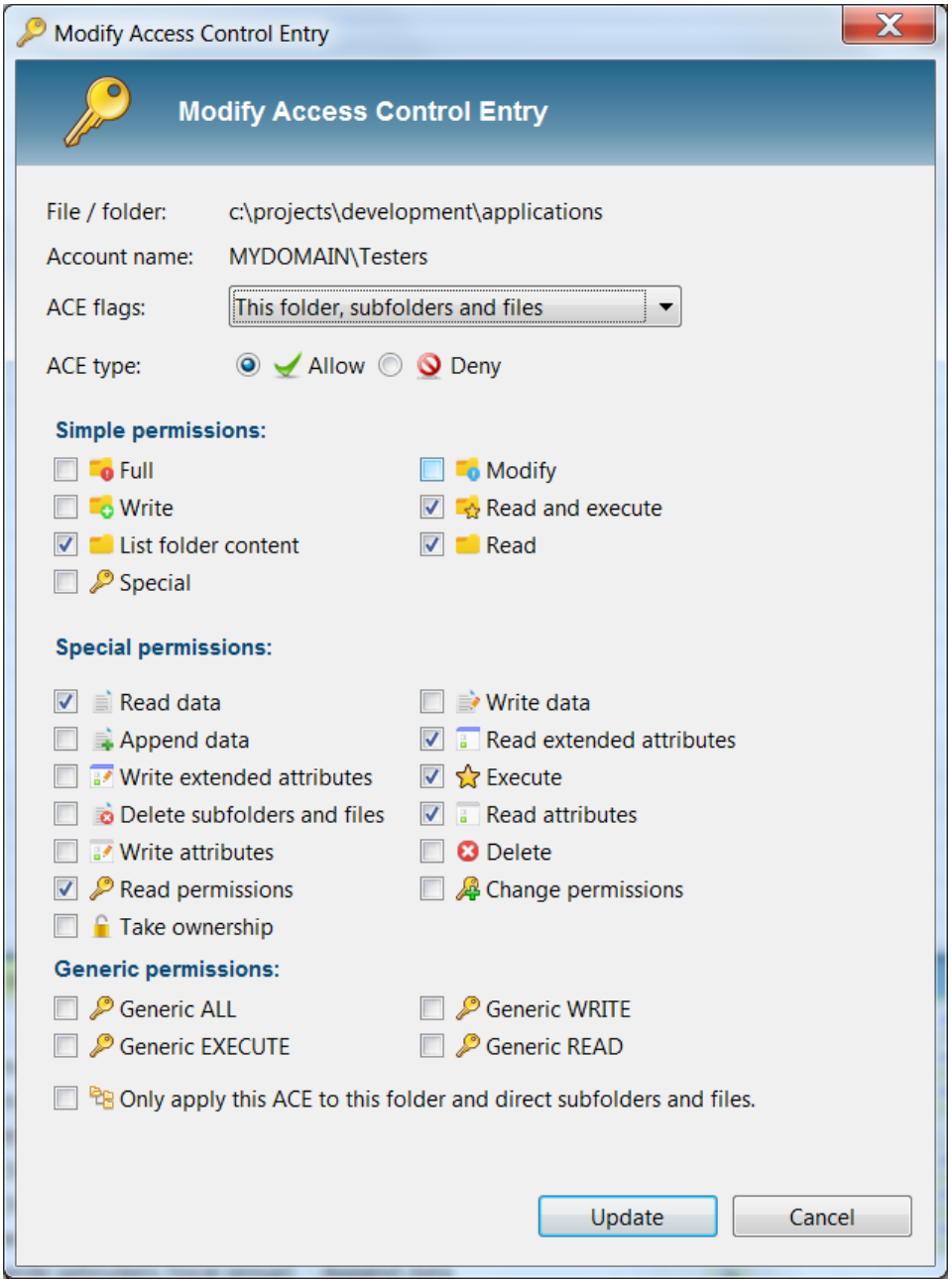
PARAMETER	FUNCTION
-scan	Automatically initiate a network scan with the current configuration, after which the application closes down. Only checked directories and LDAP OUs will be scanned. Review results of an automatic scan in the status list in Scan View or via the Last_status_messages.csv file in the application directory.
-scanDirectories	Only scans (checked) directories and files and does not change LDAP data in the database. Review results of an automatic scan in the status list in Scan View or via the Last_status_messages.csv file in the application folder.
-scanLdap	Automatically initiates a scan of all selected LDAP OUs. Directory data in the database remains unchanged.
-password	If the application is secured with a password, than this parameter, combined with a scan or report parameter, can be used to initiate the application.
-report	Exports a specific report (by name) and can include sending out an e-mail notification. Multiple reports can be exported by inputting the parameter several times: -report “All permissions for John Doe” -report “All explicit permissions in the projects folder”.
-allReports	Exports all reports and sends out all required e-mails if that option has been enabled for a report. Export files are automatically overwritten.
-allPolicies	Exports all reports with an *E-mail file/folder count threshold* value higher than 0.

MODIFYING PERMISSIONS

Change the permissions of a directory directly from within the application. Changes are directly applied to the file system and the database is updated with the changes made.

At the bottom of the search result screen is a tab that allows you to review and modify the Access Control List (ACL) of the selected directory or file. The ACL view corresponds to the **Security tab** in Windows' file properties. Permission Analyzer in some cases will show more items in the ACL, as Windows does not show generic permissions. You will be able to only show Access Control Entries (ACE) that meet the filter criteria by ticking the checkbox "Apply filter on ACL list". In addition the ACL view toolbar contains a button to directly highlight selected ACE on the file system. Permission Analyzer uses the same Windows mechanisms as the Security tab. When modifying permission through Permission Analyzer, however, information in the database is modified immediately.





DATA PROTECTION

Permission Analyzer can be secured with an application password. The password is required to open up the application and may be used to encrypt the local database using strong AES encryption.

All Permission Analyzer settings (such as LDAP connections) are automatically saved using an encryption with a built-in hidden* key. Users, however, can opt to protect their settings and access to the application with their own passwords. The application will subsequently only be accessible after start up once the correct password is entered.

Passwords themselves are not saved; only a 'one-way' hash code of the password is stored. Permission Analyzer uses an advanced hash algorithm (**PBKDF2WithHmacSHA1**), making it impossible to crack or retrieve passwords.

Alternatively, you can also choose to encrypt the local database completely with both your own password as well as an **AES** encryption. This will however result in database interaction becoming 2.5 times slower.

Please keep in mind that if you encrypt the application with a password, you will have to enter the password when running automatic scans or have reports exported via Windows Scheduled Tasks. Use the application parameter ***-password mypassword***.

* Permission Analyzer's application code is encrypted and it is very difficult, but not impossible, to retrieve textual values, such as a built-in password.

EXTERNAL DATABASE

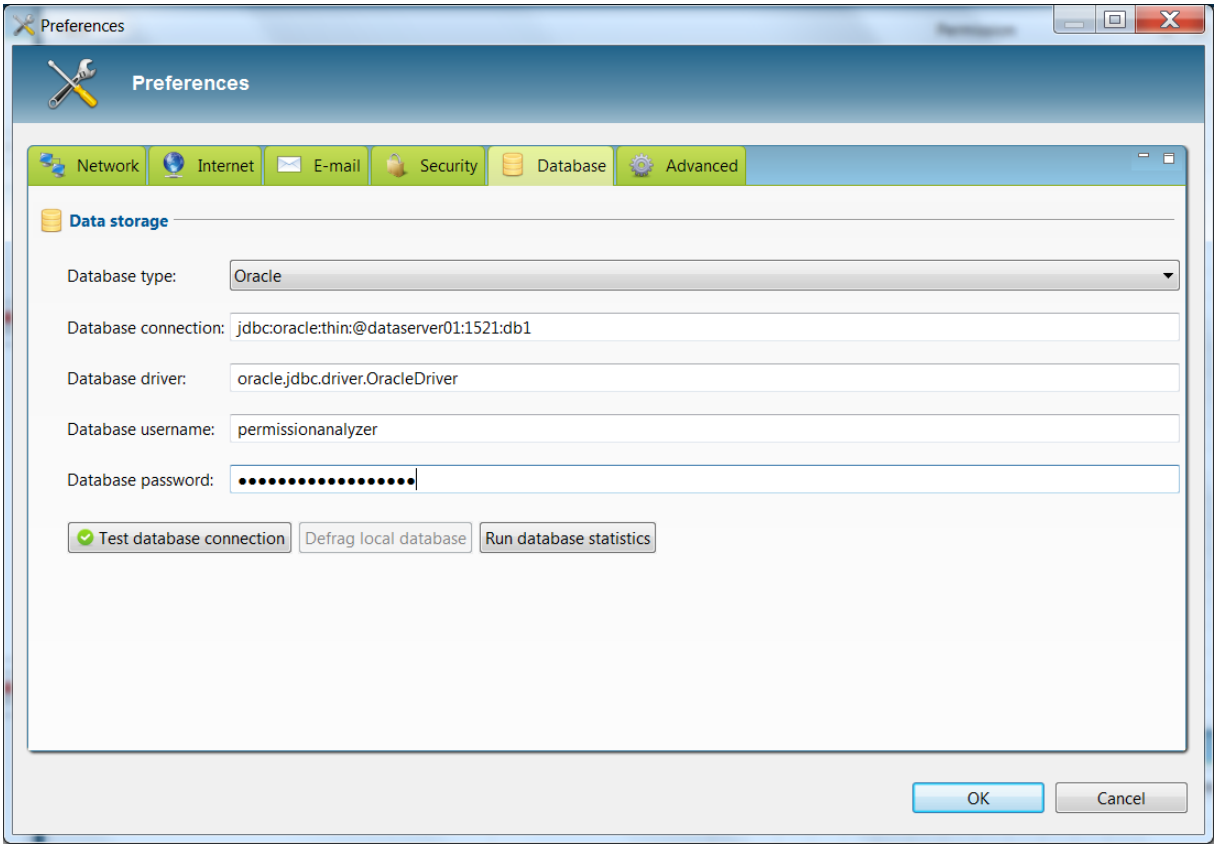
Permission Analyzer is supplied with an embedded database to store directory and group membership information. It supports a central company database, so that workstations can use the same information source or so you can create your own queries and integration.

Although Permission Analyzer is supplied with a local database (H2), which is simply a file in the application directory, you can choose to use a central database to share, say, scanned information, between installations of Permission Analyzer or to run your own queries on the database. Permission Analyzer supports Oracle, DB2, MS SQL, MySQL, PostgreSQL, Derby and H2. Please note that this feature is only supported by the **Enterprise** and **Consultant** editions.

First download the Driver Pack and overwrite the External_DB_Drivers_1.0.0.jar file in the plugins directory of Permission Analyzer. Then restart the application using the **-clean** parameter. Run one of the following SQL scripts on your central database to create the tables for Permission Analyzer:

- Oracle create script
- DB2 create script
- MSSQL create script
- MySQL create script
- PostgreSQL create script
- Derby create script
- H2 create script

Once the database has been created, open **Settings**. In the **Database** tab you will then be able to select an external database and enter the connection details.

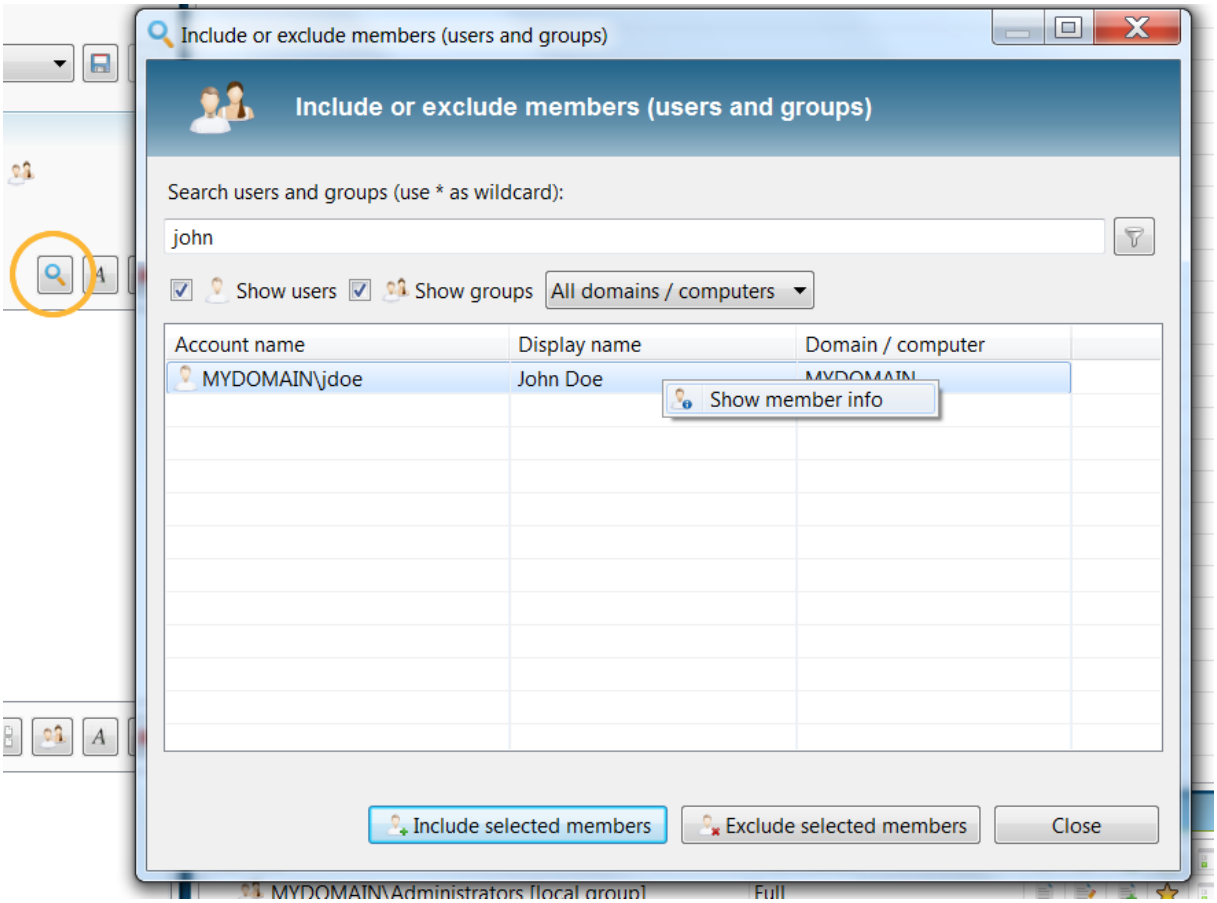


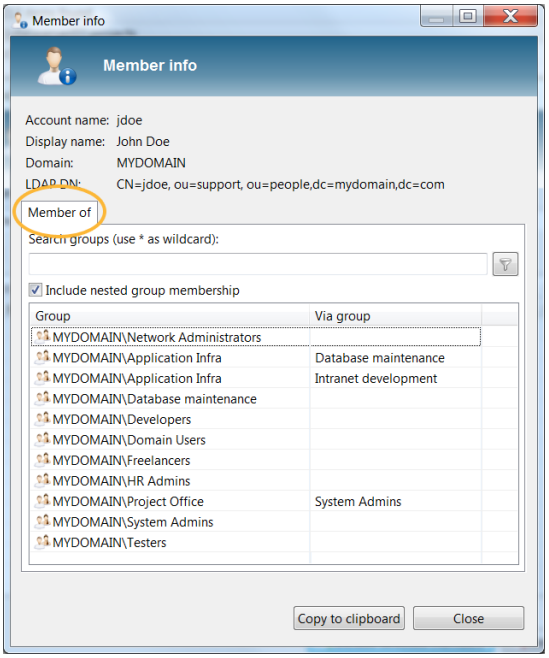
OTHER FEATURES

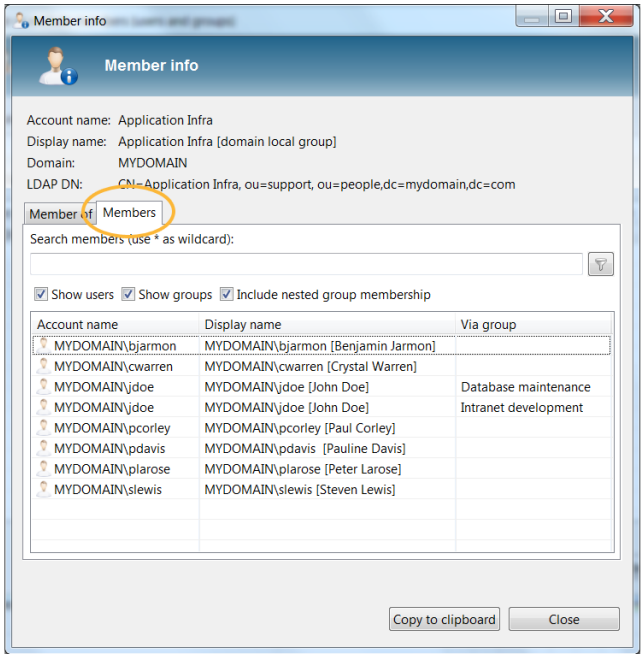
View member info and search for nested group memberships, modify LDAP attributes that are being used and make use of the update service delivered by Permission Analyzer.

Show member info

You will be able to request the details of a member or group at various points throughout the application: in the ACL view, Trace view, Member filters or search window for member selection. The member dialogue window shows both **memberOf** data as well as the **members** in the case of a group. In both cases **nested** memberships will also be shown.

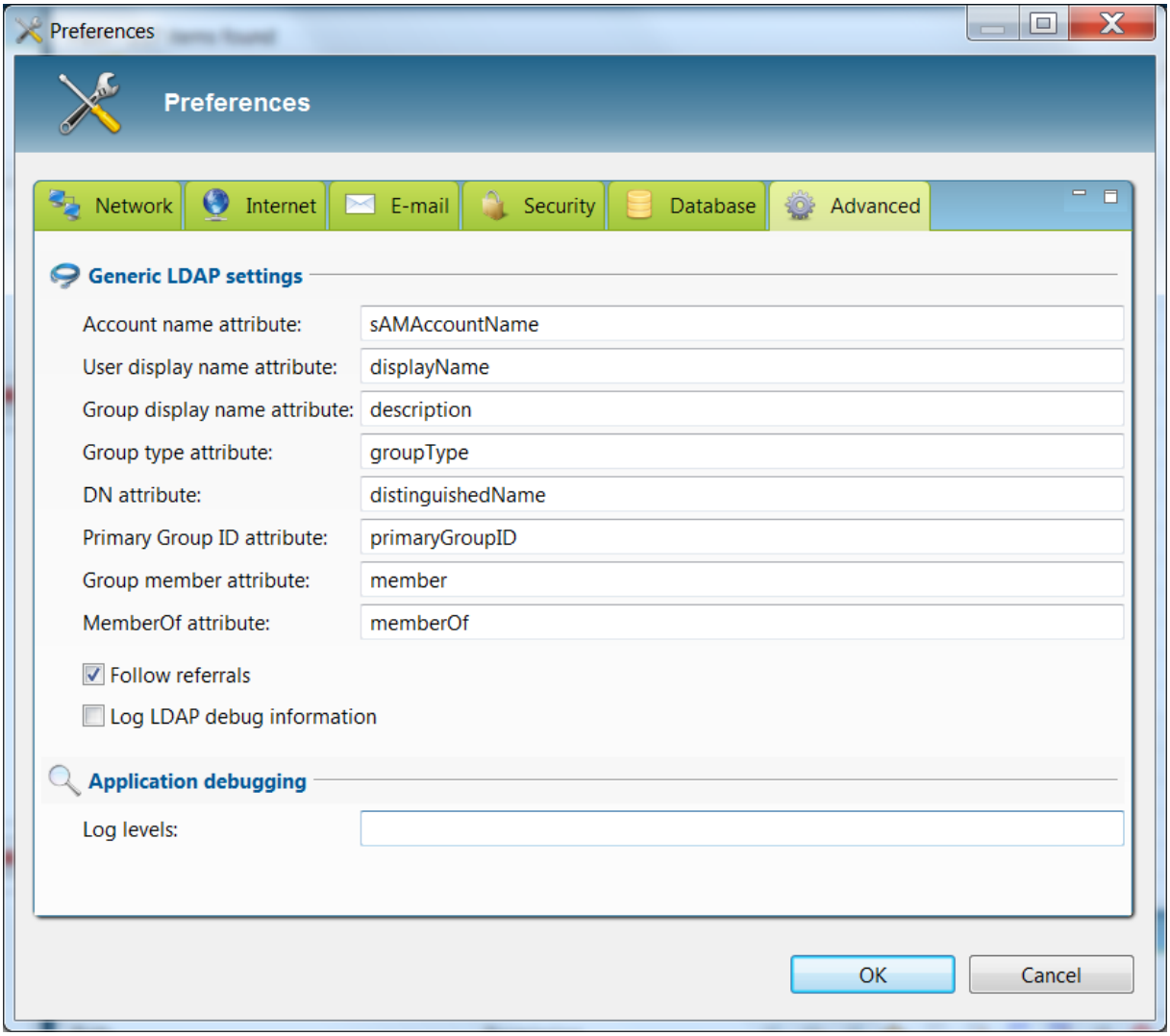

Include or exclude members (users and groups)
Include or exclude members (users and groups)
Search users and groups (use * as wildcard):
john
Show users
Show groups
All domains / computers
Account name
Display name
Domain / computer
MYDOMAIN\jdoe
John Doe
Show member info
Include selected members
Exclude selected members
Close


Member info
Member info
Account name: jdoe
Display name: John Doe
Domain: MYDOMAIN
LDAP DN: CN=jdoe, ou=support, ou=people,dc=mydomain,dc=com
Member of
Search groups (use * as wildcard):
Include nested group membership
Group
Via group
MYDOMAIN\Network Administrators
MYDOMAIN\Application Infra
Database maintenance
MYDOMAIN\Application Infra
Intranet development
MYDOMAIN\Database maintenance
MYDOMAIN\Developers
MYDOMAIN\Domain Users
MYDOMAIN\Freelancers
MYDOMAIN\HR Admins
MYDOMAIN\Project Office
System Admins
MYDOMAIN\System Admins
MYDOMAIN\Testers
Copy to clipboard
Close


Member info
Member info
Account name: Application Infra
Display name: Application Infra [domain local group]
Domain: MYDOMAIN
LDAP DN: CN=Application Infra, ou=support, ou=people,dc=mydomain,dc=com
Member of
Members
Search members (use * as wildcard):
Show users
Show groups
Include nested group membership
Account name
Display name
Via group
MYDOMAIN\bjarmon
MYDOMAIN\bjarmon [Benjamin Jarmon]
MYDOMAIN\cwarren
MYDOMAIN\cwarren [Crystal Warren]
MYDOMAIN\jdoe
MYDOMAIN\jdoe [John Doe]
Database maintenance
MYDOMAIN\jdoe
MYDOMAIN\jdoe [John Doe]
Intranet development
MYDOMAIN\pcorley
MYDOMAIN\pcorley [Paul Corley]
MYDOMAIN\pdavis
MYDOMAIN\pdavis [Pauline Davis]
MYDOMAIN\plarose
MYDOMAIN\plarose [Peter Larose]
MYDOMAIN\slewis
MYDOMAIN\slewis [Steven Lewis]
Copy to clipboard
Close

Configuring LDAP attributes

Permission Analyzer makes use of a number of standard LDAP attributes to retrieve member information and group relations. These attributes can be modified if you wish to use other fields.



Update service

Check for updates quickly at any time via [Help] > [Check for updates].

3. Download

Permission Analyzer requires **Java 7** or higher. If you don't want to install Java, then use the distribution with an embedded Java Runtime Environment (JRE). You can check your Java version by opening up a command prompt and execute "java -version" or visit www.java.com to install it.

Permission Analyzer supports any version of Active Directory and the scan can take place from any Windows machine within your domain.

Permission Analyzer for a 64 bit JRE

Permission Analyzer for a 32 bit JRE

Permission Analyzer with embedded 64 bit JRE

Permission Analyzer with embedded 32 bit JRE

VERSION HISTORY

2.0.0 **2015-09-20**

Initial version

4. Licensing model

Permission Analyzer's licensing model operates on an installation basis and consists of a number of editions based on company size, varying in the features they offer. Each **installation** of Permission Analyzer will require a separate license. The number of users and groups per edition will constitute the maximum number to be scanned by Permission Analyzer. These numbers are the sum of the unique members found in the Access Control Lists on the file system and the LDAP Organizational Units you select to determine (nested) group membership. This does not necessarily have to encompass the entire domain, but can be limited to certain OUs. Only those members and groups will then be available to the application, supplemented by the members attributed to a directory directly.

Licenses will be valid for **1 year** and automatically entitle the purchaser to tech support and updates. A license can be moved three times by deactivating an active license and reactivating it on a new device. The Consultant edition is intended to allow use of Permission Analyzer at a variety of clients within a short period of time. In that case, one license can be used on several devices, though never at the same time. This may be useful for security audits where a consultant will install Permission Analyzer within a client's domain and deactivate the license after completing the assignment.

Permission Analyzer's **trial** version is limited to two root directories with two levels of subdirectories. If you'd like to try out one of your editions, then just fill out the trial request form.

Notes:

(1) The number of servers that are scanned on directories, files and local groups. This does not relate to the number of domain controllers.

(2) Encryption is only supported for the local H2 databases supplied with the edition. Please consult the product documentation for information on encryption of other (external) databases.

(3) You will be able to use any database with a JDBC interface. Permission Analyzer automatically supports Oracle, DB2, MS SQL, MySQL, PostgreSQL, Derby and H2. Also see External Database.

(4) A license can be deactivated within the application and can subsequently be reactivated on another device. You will be able to carry this out 3 times. The Consultant Edition can be moved 200 times and can also be used to have a temporarily license operate for multiple clients. A license must always be deactivated first before a new activation can be initiated.

TRIAL	BASIC	STANDARD
-	$ 299[99]	$ 499[99]
2 root directories	Unlimited directories	Unlimited directories
1 server [1]	1 server [1]	5 servers [1]
Unlimited users	500 users	3000 users
Unlimited groups	100 groups	1000 groups
-	-	Database encryption [2]
-	-	-
-	3 license moves [4]	3 license moves [4]
DOWNLOAD	PURCHASE	PURCHASE

ENTERPRISE	CONSULTANT
$ 699[99]	$ 1299[99]
2 directories	Unlimited directories
Unlimited servers	Unlimited servers
Unlimited users	Unlimited users
Unlimited groups	Unlimited groups
Database encryption [2]	Database encryption [2]
External DB support [3]	External DB support [3]
3 license moves [4]	200 license moves [4]
PURCHASE	PURCHASE

5. FAQ

APPLICATION QUERIES

Why does the application not start?

Access denied on the workspace directory

Permission Analyzer writes data into the directory where it has been installed. If the directory is located in Program Files, Windows may decide to block the writing operations of the application. If this is the case, run Permission Analyzer as an Administrator. Right click Permission Analyzer.exe and select Run as Administrator.

What exactly is retrieved from the Active Directory?

Permission Analyzer makes use of the Active Directory to retrieve additional member attributes that are not available from the file system, e.g. the displayName and (nested) group membership. The application's scan screen will show specific Active Directory Organizational Units (OU) to be scanned and Permission Analyzer will limit the scan to those OUs. The scan will only search for items outside the OUs if they occur in the **member** or **memberOf** attributes of members in the OU. This is done to obtain a complete overview of group membership for each member of the OU(s).

Do I have to install the product directly on a domain controller?

No, you can run Permission Analyzer from any server or workstation within your domain, as long as you have enough permissions to read the security properties of the directories to scan and the OUs in the Active Directory.

Does the application require an Internet connection?

No, you can use an Internet connection to activate your license automatically, but you can also use our form on the website to create an offline activation file based on your license.

Can I change the location of the embedded database?

Yes, just move the files **H2DB.h2.db** and **H2DB.trace.db** to another location on your hard disk and change the database path in the settings of the application.

I've discovered a bug. How can I report it?

A dialog window can be opened within the application, allowing you to send a direct message to our tech support team. The dialog window also allows you to send the application log in zip format. Go to [Help] > [Contact support]. Make sure you've configured a valid SMTP server in the application settings before sending out the e-mail.

LICENSING QUERIES

How can I move my license?

A license is linked to an installation of Permission Analyzer. That's why it's important to deactivate an old, previous installation. This can be done automatically online or manually through the website. Open [Help] > [License information] and select [Deactivate license]. You will now be able to activate the license on another device.

How many licenses do I need?

A license is needed for every installation of Permission Analyzer. You should select the appropriate addition of Permission Analyzer based on the number of groups and users you are scanning on the file system and Active Directory. If you'd like to move Permission Analyzer regularly, e.g. to use for several clients temporarily, then you're best off choosing the **Consultant Edition**.

How can I get a written quote?

Our sales agent Share-It is happy to send you a quote upon request. Prices noted in the offer are non-binding and may be subject to currency fluctuations. Quotes are valid for 14 days. If a quote is not processed as an order within this period, it will be automatically cancelled in our system.

Select the edition for which you wish to receive a quote:

- Basis Edition
- Standard Edition
- Enterprise Edition
- Consultant Edition

What is Permission Analyzer's ordering process like?

Permission Analyzer's orders are processed by our sales agent Share-It, one of the biggest software sales agents worldwide. Share-It supports the following payment methods: credit card (Visa, MasterCard, American Express, JCB and Diner's Club, as well as Maestro debit cards issued in the UK), wire transfer, check, PayPal and WebMoney. When you pay by credit card you will immediately receive the license file(s) by e-mail.

The trial version is very limited. Can I test a full version?

Sure! Just fill out our online form to request a trial license for a specific edition.

Can I sign up as a reseller?

Yes, you can register as a reseller or affiliate through our sales agent, Share-It. As an affiliate, you can market Permission Analyzer by placing links on your website to the relevant product pages on the publisher's website. You will receive a commission for each sale of these products via your website. As a reseller you will be able to quickly and easily place online orders for your customers for products by "Perdemia". As a reseller, you can log in to the publisher's website without having to re-enter your personal information for every order.

Register as affiliate
Register as reseller